Do Not Perform Arithmetic with Unvalidated Input

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03 L4 / D/P[4]

Careless modulo arithmetic can introduce vulnerability.

Description

According to [Seacord 05]:

> Integers represent a growing and underestimated source of vulnerabilities in C and C++ programs. This is primarily because boundary conditions for integers, unlike other boundary conditions in software engineering, have been intentionally ignored. Most programmers emerging from colleges and universities understand that integers have fixed limits, but because these limits were either deemed sufficient, or because testing the results of each arithmetic operation was considered prohibitively expensive, violating integer boundary conditions has gone almost entirely unchecked in commercial software.

For an indepth coverage of this issue in C and C++, see Safe Integer Operations[7].

References

[Blexim 02]	blexim. *Basic Integer Overflows*. http://www.phrack.org/phrack/60/p60-0x0a.txt (2002).
[Hoglund 04]	Hoglund, Greg & McGraw, Gary. *Exploiting Software: How to Break Code.* Boston, MA: Addison-Wesley, 2004.
[Horovitz 02]	Horovitz, Oded. *Big Loop Integer Protection*. http://www.phrack.org/phrack/60/p60-0x09.txt (2002).
[Howard 03a]	Howard, Michael. *Reviewing Code for Integer Manipulation Vulnerabilities*. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure04102003.asp (2003).
[Seacord 05]	Seacord, Robert C. *Secure Coding in C and C++*. Boston, MA: Addison-Wesley, 2005.
[Thompson 05]	Thompson, Herbert & Chase, Scott. *The Software Vulnerability Guide*. Charles River Media, 211-222. 2005.

Carnegie Mellon Copyright

3. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/320-BSI.html (Fithen, William L.)
7. http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/coding/312-BSI.html (Safe Integer Operations)
1. mailto:permission@sei.cmu.edu

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.